CANADIAN PRIVACY LAW REVIEW

Volume 2 • Number 7 April 2005

ONTARIO HEALTH PRIVACY

LexisNexis® Butterworths

E. Michael Power
Partner
Gowling Lafleur Henderson LLP, Ottawa

Louis Benoit
Associate
Gowling Lafleur Henderson LLP, Ottawa

Ontario & Health Information Privacy: Legislation Finally Arrives

After failed attempts in 2000 and 2002, Ontario has become the latest Canadian province to enact personal health information protection legislation. The *Personal Health Information Protection Act*[1] (PHIPA) came into force on November 1, 2004 and creates a regime of information practices pertaining to the collection, use or disclosure of personal health information. The legislation applies to all health information custodians within the province of Ontario and to individuals and organizations that receive personal health information from health information custodians. The Act "codifies" certain traditional obligations of health practitioners while introducing some new concepts. This brief article is intended to serve as an introduction to some of the more "distinctive" elements of PHIPA.

"Personal Health Information" is…

As is the case with other privacy statutes in Canada, personal health information (PHI) is described broadly[2] as identifying information about an individual in oral or recorded form. It includes information that relates to (i) the physical or mental health of the individual (including the health history of the individual's family), (ii) the provision of health care to the individual, (iii) payments or eligibility for health care in respect of the individual, and (iv) the donation by the individual of any body part or bodily substance or is derived from the testing or examination of any such body part or bodily

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

ISBN 0-433-44417-7 ISSN 1708-5446
ISBN 0-433-44418-5 (print & PDF)
ISBN 0-433-44650-1 (PDF)
ISSN 1708-5454 (PDF)

Subscription rates: $175.00 plus GST (print or PDF)
$274.00 plus GST (print & PDF)

substance. It also includes an individual's health number, and the identity of an individual's substitute decision-maker. Any other information about an individual found in a record containing personal health information is also captured within the meaning of PHI. However, employee records of a custodian are excluded from the definition provided that the records are used primarily for purposes other than providing health care.

Health Information Custodians under PHIPA

- Health care practitioners.
- Service providers under the *Long-Term Care Act*.
- Community care access corporations.
- Operators of hospitals, psychiatric facilities, mental health institutions or independent health facilities.
- Nursing homes, special care homes & homes for the aged.
- Pharmacies.
- Laboratories.
- Ambulance services.
- Community health or mental health centres.
- Evaluators or assessors under specific consent and capacity statutes.
- The Ministry of Health and Long-Term Care.

Held by Health Information Custodians…

The Act does not apply to all personal health information, but only that which is collected, used and disclosed by health information custodians.[3] The term "health information custodian" (the "custodian") has an extensive definition and covers those who have the custody or control of PHI in connection with their powers or duties.

PHIPA imposes obligations on custodians to notify their clients of the theft, loss or unauthorized access of their PHI.[4] Custodians may also be subject to civil actions for damages, including a maximum of $10,000 for mental anguish and fines of up to $50,000 if the custodian is an individual or $250,000 if the custodian is a corporation.[5]

PHIPA also clarifies some of the ambiguities that existed under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)[6] with respect to the application of privacy principles such as consent and disclosure in the course of providing health care services.

Involving Different "Flavours" of Consent…

PHIPA provides consent procedures that are fairly simple and workable. All consents must be knowledgeable, meaning that it must be reasonable to believe that the individual knows the purposes for the collection, use or disclosure of his or her information.[7] Generally, implied consent is sufficient in the course of providing health care if a poster or brochure is readily available

and likely to be seen by a client which explains these purposes.[8] PHIPA also states that where a custodian receives PHI from an individual for the purposes of providing health care to that individual, the custodian may assume that it has the individual's consent to disclose that information to another custodian for such purposes.[9]

However, if a custodian wishes to disclose PHI to someone who is *not* a custodian, then the individual's express consent must be obtained.[10] This may be the case, for example, where PHI is requested by an insurance company or an employer. Nonetheless, a custodian may disclose personal health information without consent where the custodian believes on reasonable grounds that the disclosure is necessary to eliminate or reduce a significant risk of bodily harm to one or more persons.[11]

Where There is No Capacity to Consent…

PHIPA provides that an individual is capable of consenting to the collection, use or disclosure of personal health information if the individual is able to understand the relevant information and the consequences of giving or withholding consent.[12] A custodian may presume the individual is capable, unless there are reasonable grounds to believe that the individual is incapable of consenting.[13]

Where an individual cannot provide consent, the custodian must provide to the individual with information about the consequences of this determination and the individual may apply to the Consent and Capacity Board for a review of the determination of incapacity.[14] Generally, a parent may consent on behalf of a child who is less than 16 years of age.[15]

"Substitute" Consent Providers

Where there is no capacity to provide consent, the following, in descending order, may do so on behalf of an individual:

- a guardian of the person or guardian of property;
- an attorney for personal care or attorney for property;
- a representative appointed by the Consent and Capacity Board;
- a spouse or partner;
- a child or parent of the individual;
- a brother or sister; or
- any other relative.

"Locking" PHI…

PHIPA provides that an individual may request that a custodian not disclose all or certain elements of his or her personal information to another custodian.[16] In such a case, the disclosing custodian must inform the recipient custodian that some PHI is inaccessible since it has been "locked" by the individual.[17] This principle is somewhat controversial in that it allows patients the right to permit the collection, use and disclosure of only some of their personal health information, potentially reducing the effectiveness of health care treatment as a result of inadequate disclosure to the applicable health care provider.[18]

Fundraising is Protected…

PHIPA also addresses the collection, use and disclosure of personal information in the context of fundraising activities. The Act states that a custodian may rely on implied consent for the collection, use and disclosure of personal information for fundraising purposes, but *only* if the information is limited to the name and contact information of the individual. Where the information includes more than just name and contact information, the custodian must obtain express consent.[19]

However, a custodian may not collect, use and disclose PHI for marketing or market research purposes unless the individual expressly consents to such purposes.[20]

As is Research…

PHIPA permits custodians to use and disclose PHI for research purposes, without an individual's consent, if certain requirements are met. For example, a custodian who uses PHI for research purposes and a researcher who seeks disclosure of PHI for research purposes must both submit a detailed research plan to a research ethics board for approval.[21]

The regulations contain certain requirements with respect to research ethics boards. For example, a research ethics board must have at least five members, including one member with no affiliation with the person that established the research ethics board, one member knowledgeable in research ethics, two members with expertise in the methods or in the areas of the research being considered, and one member who is familiar with privacy issues.[22]

The Act requires that a research plan set out the affiliation of each person involved in the research, the nature and objectives of the research and the anticipated benefits of the research.[23] The regulations also contain a list of additional items that must be present in a research plan, including a description of the PHI required and the potential sources, a description of how the PHI will be used, an explanation as to why the research cannot reasonably be accomplished without the PHI, an explanation as to why consent to the disclosure of the PHI is not being sought, a list of all persons who will have access to the information and their roles in the research project and a description of the safeguards that the researcher will impose to protect the confidentiality and security of the PHI.[24]

The Act also stipulates that in deciding whether or not to approve the research plan, the research ethics board must consider whether the objectives of the research can reasonably be accomplished without using the PHI, whether adequate safeguards will be in place to protect the privacy and confidentiality of the individuals and their PHI, the public interest in conducting the research and in protecting the privacy of the individuals whose PHI is being disclosed, and whether obtaining the consent of the individuals would be impractical.[25]

A researcher that requests PHI must submit to the custodian a written application, a research plan and a copy of the decision approving the research plan by the research ethics board. The custodian must enter into an agreement with the researcher before disclosing PHI.[26]

And Risk Management…

The Act allows a custodian to use PHI for the purposes of risk management, error management or for the purpose of activities to improve or maintain the quality of care or the quality of any related programs or services of the custodian.[27] The regulations also specify that an agent who has received PHI from a custodian for the purposes of risk management and error management, may use that information, together with other such information that the agent has received for these same purposes, from other custodians, for the purposes of general risk management analysis if the agent is the Canadian Medical Protective Association or the Healthcare Insurance Reciprocal of Canada, and the agent does not disclose PHI provided to it by one custodian to another custodian.[28]

Use of Health Card Numbers…

PHIPA prohibits individuals or organizations who are not custodians from collecting or using a health card number, except where it is related to the provision of provincially-funded health resources, for purposes which a custodian has disclosed the number to the individual or organization, or for health-related purposes (*e.g.*, regulating health professionals, health planning and administration, health research or epidemiological studies).[29]

Non-custodians cannot disclose a health card number, except as required by law.[30] Permitted instances of disclosure are set out in the regulations,[31] including for purposes related to the provision of provincially-funded health resources and for certain research-related purposes.

Only individuals or organizations that provide provincially-funded health services can require individuals to produce their health cards.[32]

Non-Custodians Captured to a Certain Degree…

PHIPA also has limited application to individuals or entities who are not custodians in that where a custodian discloses PHI to a non-custodian, that individual or entity may only use or disclose the information for purpose(s) authorized by the custodian.[33] It is also important to note that where a custodian discloses PHI to an agent, PHIPA treats such disclosure as a *use* by both the custodian and the agent and not a *disclosure* by the custodian or a collection by the agent.[34] The Act restricts the agent to the collection, use, disclosure, retention or disposal of the information, as the case may be, only in the course of the agent's duties as agent to the custodian.[35]

As are Service Providers…

A person who provides goods or services to enable a custodian to electronically collect, use, modify, disclose, retain or dispose of PHI, is a "service provider" and faces certain obligations under PHIPA.[36]

A service provider shall notify every custodian — at the first reasonable opportunity — in the event of unauthorized access to the PHI. It also has to provide each custodian with a description of the services, in a form that is appropriate for sharing with the individuals

to whom the PHI relates, including a general description of the safeguards in place to protect the PHI. In addition, the service provider has to make available to the public:

- the service description;
- any appropriate service-related directives, guidelines and policies; and
- a general description of the safeguards in relation to the security and confidentiality of the information.[37]

Service Providers

- May only use PHI to provide contracted services.
- Must make certain information available to the public.
- Cannot disclose PHI.
- Cannot permit employees or agents to access PHI unless they agree to comply with same restrictions.

Other Obligations…

PHIPA contains other obligations that are similar in nature to those found in other Canadian privacy statutes. Custodians are required to establish and comply with information practices in order to respect their obligations within the Act.[38] Every custodian must designate a contact person who is authorized to facilitate the custodian's compliance with this Act, respond to inquiries from the public about the custodian's information practices and respond to requests for access and complaints.[39] Also, each custodian must make available to the public a written statement that provides a general description of the custodian's information practices, describes how to reach the contact person and how an individual may access, correct or make a complaint regarding their PHI.[40] If a custodian uses or discloses personal health information about an individual, without the individual's consent, in a manner that is not described in the custodian's statement the custodian has to inform the individual of the uses and disclosures at the first reasonable opportunity, make a note of the uses and disclosures, and keep the note as part of the PHI records about that individual.

Custodians must take reasonable steps to ensure that the information they maintain about an individual is as accurate, complete and up-to-date as is necessary for their required purposes.[41] PHIPA also requires each custodian to address information security by taking reasonable measures to ensure that PHI in their control is protected against theft, loss and unauthorized use or disclosure and to ensure that the information is protected against unauthorized copying, modification or destruction.[42]

To Conclude…

Health practitioners are familiar with the requirement to maintain the confidentiality of patient information. To the extent that PHIPA complements this traditional obligation, most custodians should not find some of the concepts in this legislation to be unusual or particularly burdensome. The extensive provisions pertaining to collection, use and disclosure without consent for health care purposes preserve the essential elements of current practices in Ontario today. Some new aspects (*e.g.*, access) and a greater emphasis on others (*e.g.*, security) may raise concerns amongst custodians. However, these obligations reflect the increasing sensitivity of individuals to the treatment of their personal health information and are not so different from those being applied generally to businesses through PIPEDA or applicable provincial statutes.

---

1 S.O., 2004, c. 3, Sch A.
2 See, s. 4.
3 Section 7(1).
4 Section 12(2).
5 Sections 65(3) and 72(2).
6 S.C. 2000, c. 5.
7 *Supra*, note 1, s. 18(5).
8 Section 18(6).
9 Section 20(2).
10 Section 18(3).
11 Section 40(1).
12 Section 20(1).
13 Sections 21(4) and (5).
14 Sections 22(2) and (3).
15 Section 23(1).
16 Section 19(2).
17 Sections 20(3) and 38(2).
18 This is an issue that was discussed in length during Legislative Assembly debates on the Bill. See for example, the March 30, 2004 debates at: <http://www.ontla.on.ca/hansard/house_debates/38_parl/Session1/L023B.htm>.
19 *Supra*, note 1, s. 32(1).
20 Section 33.
21 Section 44(1).
22 O. Reg. 329/04, s. 15.
23 *Supra*, note 1, s. 44(2).
24 O. Reg. 329/04, s. 16.
25 *Supra*, note 1, s. 44(3).
26 Section 44(1).
27 Section 37(1)(d).
28 O. Reg. 329/04, s. 7.
29 *Supra*, note 1, s. 34(2).
30 Section 34(3).
31 O. Reg. 329/04, s.12.
32 *Supra*, note 1, s. 34(4).

[33] Section 49(1).
[34] Section 6(1),
[35] Section 17.
[36] O. Reg. 329/04, s. 6(1).
[37] O. Reg. 329/04, s. 6(3).
[38] *Supra*, note 1, s. 10(1).
[39] Section 15.
[40] Section 16(1).
[41] Section 11.
[42] Section 12(1).

INTERNATIONAL DEVELOPMENTS

US Privacy Law Update

by Julie O'Neill
Collier Shannon Scott PLLC
Washington, DC

Editor's note: Ms. O'Neill's photo was unavailable at time of publication.

Commercial E-mail: Regulatory Focus on Affiliate Marketing

- In the last two-and-a-half months, the Federal Trade Commission (FTC) has used a provision of the *CAN SPAM Act* that allows for the prosecution of both an affiliate marketer and the company whose product or service it markets. Under that provision, a company that uses a third party marketer is liable for the marketer's violations of the Act if it knew or should have known of the violations, profited from the affiliate's e-mail promotion and took no action to prevent the violations or to detect them and report them to regulators. In mid-January, the Commission sued a network of companies and individuals who marketed pornography Web sites by e-mail, alleging that their messages did not comply with the Act's disclosure, labeling, opt-out and other requirements. Interestingly, just one of the defendants — the affiliate marketer — actually sent the unlawful messages. The FTC charged the others because they paid the marketer to send the e-mails on their behalf, and they profited from his promotions. According to the Commission, the defendant Web site owners knew or should have known that the messages transmitted on their behalf violated the law, and, for this reason, they were as liable for the violations as the actual sender. Similarly, at the end of March, the FTC settled charges that the seller of an allegedly bogus diet patch had violated the *CAN SPAM Act* by having its affiliate marketers send messages on its behalf. The Commission originally filed suit against the seller back in April 2004. The seller responded that it could not be held liable because the FTC could not prove that it sent the offending messages. In July, a U.S. District Court judge supported the FTC's position, finding that liability "...is not limited to those who physically cause spam to be transmitted, but also extends to those who 'procure the origination' of offending spam" (*FTC v. Phoenix Avator, LLC*, 2004 U.S. Dist. LEXIS 14717). The court also found that the Commission had gathered a "persuasive chain of evidence" connecting the seller to the alleged violations. The settlement ends the litigation with a stipulated order that, among other things, prohibits the defendants from future violations.

Do-Not-Call

- In mid-February, the FTC announced its first do-not-call rule settlements. In those cases, the Commission settled charges that two timeshare sellers and their telemarketers had violated the rule by, among other things, calling thousands of consumers who had placed their phone numbers on the national do-not-call registry. The FTC alleged that the timeshare sellers were liable not only for their own unlawful calls, but also for hiring telemarketers to place calls that violated the rule. The settlement with the timeshare sellers imposes a variety of injunctive relief and requires them to pay a $500,000 civil penalty. A similar penalty imposed on the telemarketers was reduced to $3,500, based on their demonstrated inability to pay. They, too, are subject to a variety of injunctive provisions.

FTC Reports

- **Spyware:** In early March, the Commission released a report summarizing the issues raised at — and reaching some conclusions from — its April 2004 spyware workshop. The Commission concluded that spyware is a real problem that can result in serious privacy and security risks for consumers. It also concluded that these risks can be reduced if both the government and the private sector take certain actions. It recommended that industry: (1) develop standards for defining "spyware"; (2) educate consumers about it; (3) develop technological solutions to protect consumers against

the risks associated with it; and (4) assist law enforcement with their efforts to combat spyware. The Commission also suggested that government: (1) increase civil and criminal prosecution of spyware distributors under existing laws; (2) increase efforts to educate consumers about spyware's risks; and (3) encourage industry to develop technological solutions.

- **RFID:** Also in early March, the Commission issued a report from its June 2004 workshop on radio frequency identification (RFID). While the Commission acknowledged that the use of RFID technology can offer businesses and consumers significant benefits, it noted that some applications raise privacy concerns — for example, by monitoring consumer behaviour without adequate notice and consent. Based on the workshop and comments it received from interested parties, the FTC reached a number of conclusions, including that: (1) industry initiatives have a vital role in addressing the privacy issues associated with certain RFID uses; (2) the goal of such initiatives should be transparency; (3) any self-regulatory program established by industry should include provisions designed to ensure compliance; (4) companies that use RFID to collect personal information must implement measures to protect such information; and (5) industry, government and privacy advocates should work together to educate consumers about RFID technology and the choices they have with respect to its use.

Information Security

- In response to several recent, highly-publicized data security breaches at large companies (including the theft of personally identifiable information from data aggregator ChoicePoint), federal lawmakers have been holding hearings to determine what, if any, legislation to introduce. Several members of Congress and some industry groups have called for national legislation requiring companies to notify affected individuals of security breaches. One lawmaker plans to propose a bill that would create federal data protection standards and require corporate officers to attest that their companies comply with them. Another proposed bill would require companies to notify affected individuals in the event that their personal information is compromised as the result of a database breach. This proposal mirrors the requirements of California's database breach notification act, which is currently the only U.S. requirement that consumers be informed that their information may have been stolen.
- Under new rules issued by federal bank regulators, financial institutions must immediately report database security breaches to their regulators and to law enforcement agencies. The rules also require financial institutions to notify their customers of such breaches, but only if the financial institution determines that the personal information is likely to be misused. Bank regulatory agencies are expected to develop notification guidelines within the next few months.

European Privacy Law Update

Christopher Kuner
Partner
Hunton & Williams LLP, Brussels, Belgium

International Developments

European Union and Asia Unite against Spam

On February 21-22, 2005, government representatives attended the fourth ASEM Conference on E-Commerce in London. ASEM is a multilateral forum for action-orientated debate between the 25 EU Member States, the European Commission, and 13 Asian partner countries. In a joint statement, ASEM delegates agreed to take action to fight spam nationally and to promote international anti-spam cooperation. ASEM members include China and South Korea, which are reportedly major sources of spam. EU Information Society and Media Commissioner Viviane Reding welcomed the initiative. Further information on ASEM, along with the Newsletter of the fourth annual conference, is available at: <http://www.asemec-london.org>.

European Union Developments

Internal Market Commissioner Welcomes Payment Industry Strategy

In early February 2005, the Article 29 Working Party endorsed the final version of the "Guidelines for Terminated Merchant Databases" negotiated between the European Commission and the payment industry. The Guidelines are designed as an instrument of best practice. They set forth the conditions under which payment systems, banks, payment services providers, associations and other participants established on the territory of one or more EU Member States may operate cross-border databases containing the data of merchants which have been terminated from participating in their systems. The final document is the result of negotiations between the payment industry and the Working Party that stretched over two years. The Working Party is to monitor implementation of the guidelines, and a first review of the Guidelines is scheduled in early 2006.

On March 2, 2005, Internal Market Commissioner Charlie McCreevy released a statement supporting the guidelines. The document identifies the financial institutions that were involved in the negotiations, namely Visa Europe and MasterCard Europe, emphasizing their commitment to comply with data protection rules.

See Press Release of the European Commission at: <http://www.europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/246&format=HTML&aged=0&language=EN&guiLanguage=en>; the Guidelines, along with their annexes, can be consulted at: <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/others/2005-01-11-fraudprevention_en.pdf>.

EU Commission Approves Alternative Standard Contractual Clauses for Data Transfers

On December 27, 2004, the European Commission granted final approval to the industry alternative model clauses for controller-to-controller transfers of personal data; the clauses may therefore be used to ensure an adequate level of data protection for transfers from the EU as from April 1, 2005. The Commission's existing controller-to-controller contracts of 2001 will remain in effect, so that data exporters will have two sets of clauses to choose from. The seven business groups that proposed the clauses for approval were led by ICC Data Protection Task Force Chairman Christopher Kuner of Hunton & Williams' Brussels office.

FAQs explaining some of the differences between the new clauses and the existing Commission clauses are available on the ICC Web site at: <http://www.iccwbo.org/home/news_archives/2005/data_transfers.asp>.

Commission Decision C(2004)5271 approving the alternative standard contractual clauses for the transfer of personal data to third countries was published in Official Journal L 385 of December 29, 2004. It is available in all languages of the European Union. The English version can be accessed at: <http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf>.

Article 29 Working Party : Latest Developments

During its session of January 18 and 19, 2005, the Article 29 Working Party adopted the following documents:

- Working Document 104 on data protection issues related to intellectual property rights: see <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp104_en.pdf>; and
- Working Document 105 on data protection issues related to RFID technology: see <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf>.

  Simultaneously, the Working Party launched a public consultation on each document. Interested parties are encouraged to submit their comments by March 31, 2005. Contributions should be sent to the following address: <markt-privacy-consultation@cec.eu.int>.
- Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record (PNR) and Advance Passenger Information from airlines. The Opinion concludes that Canada does provide an adequate level of data protection for PNR data. It is available on the Working Party's Web site, at: <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp103_en.pdf>.

On February 23, 2005, the Working Party released a report adopted on January 18, 2005 on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification, and the role of the data

protection officers in the European Union; the full report is available in English at: <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp106_en.pdf>.

The Article 29 Working Party also published its seventh report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the years 2002 and 2003, available at: <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/7th_report_prot_individs_en.pdf>.

European Commission Data Protection Unit to Move to DG Justice

A decision has been made in the upper levels of the European Commission to move the Data Protection Unit, which is presently located in Directorate-General (DG) Internal Market, to the DG Freedom, Security and Justice. The decision was to be announced on February 16; it has apparently not yet been decided how to integrate the unit into the new DG, or who will staff it.

Recent Developments in EU Member States

France: CNIL Simplifies Notification Procedure for HR Data Processing

In its plenary session on January 13, 2005, the French data protection authority (CNIL) adopted a new simplified procedure for notifying the processing of personal data, which will in particular simplify the notification of human resources data, as well as make it possible to conduct notifications online.

Both private and public data controllers will benefit by the simplification, which covers data processed in connection with personnel administration (such as professional data, directories, etc.), the use of electronic tools (follow-up and maintenance of hardware, e-mail, intranet), work organization (professional diaries, task managers), and career management (evaluation, mobility, trainings). Sensitive data such as medical, social security or biometric data, or data that may be used for the purpose of monitoring employees, are not covered.

For further information, consult the CNIL Web site: <www.cnil.fr> (in French only).

France: Fifth Edition of Big Brother Awards

The fifth edition of the French Big Brother Awards ended on January 21, 2005, on the 50th anniversary of the death of writer George Orwell. During the closing ceremony, held under the auspices of Privacy International, a jury of ten citizens, composed of academics, human right campaigners, lawyers, magistrates, writers and filmmakers, honoured publicly the best "ambassadors of the surveillance society" in 2004. Further information, including a presentation of the winners, is available, in French and English, at: <http://www.bigbrotherawards.eu.org/2004/presse.php>.

France: Opt-out Becomes the Rule for B2B Marketing

During its February 17, 2005 session, the French data protection authority (CNIL) reversed its position on e-mail direct marketing in the B2B context: the CNIL stated that the sending of a commercial message to an individual's professional e-mail account and for professional purposes is no longer subject to the individual's prior consent. Until then, the CNIL had favoured a strict interpretation of the law, considering that the opt-in requirement applicable to e-mail marketing also applied to individuals acting in their professional capacity. However, since the purpose of the opt-in rule is to protect consumers, not to adversely affect exchanges between businesses, it decided that opt-out should become the rule in the B2B context.

For further information (in French only), consult the CNIL Web site: <http://www.cnil.fr/index.php?id=1780&news[uid]=238&cHash=6dd2646505>.

Germany: Federal Commissioner Issues Guidance on Internet Use in the Workplace

On March 8, 2005, the German federal data protection commissioner, Peter Schaar, who is also Chairman of the Article 29 Working Party, published a flyer on employee use of the Internet in the workplace. The principles are applicable both in the private and public sector. The Guidelines can be downloaded free of charge from the Internet (in German only) : <http://www.bfd.bund.de/information/flyer_net.pdf>.

The Netherlands: Dutch Regulator Imposes Record Fines on Spam

On December 28, 2004, OPTA (the Dutch independent post and telecommunications regulatory authority) imposed fines totaling a record € 87,500 (app. US$110,000) against individuals and small companies for sending unsolicited e-mail and SMS messages.

The heaviest fine of € 42,500 (app. US$55,000) was imposed on an individual, whose identity has not been revealed, for sending four spam messages. In one of them, he advertised an edition of Adolf Hitler's book *Mein Kampf* under the identity of the Dutch anti-spam expert Rejo Zenger. Another spam involved the sale of pharmaceutical products over the Internet.

OPTA was reacting to numerous complaints that have been collected on a special spam Web site since May 2004: see <www.spamklacht.nl>. An OPTA spokesman admitted that OPTA has no authority to fight spam originating outside the Netherlands. See press release (in Dutch): <http://www.opta.nl/asp/nieuwsenpublicaties/persberichten/document.asp?id=1506>.

UK: Consumer Group Calls for Boycott of Supermarket Chain over Use of RFIDs

On January 25, 2005, consumer group Caspian (Consumers Against Supermarket Privacy Invasion and Numbering) launched a boycott of Tesco supermarkets in the UK because of Tesco's plan to affix Radio Frequency Identification (RFID) tags on individual products. The announcement was made live on BBC television, thus reaching millions of viewers. Caspian called on consumers to boycott the chain until the practice is stopped. For background information, visit this Web site: <http://www.spychips.com/boycotttesco/>.

PIPEDA FINDINGS

Michael Geist
Editor-in-Chief of the *Canadian Privacy Law Review*. Research Chair in Internet and E-Commerce Law, University of Ottawa.

Candice Teitlebaum
Student-at-law
Aird & Berlis LLP, Toronto

Recent Health Information PIPEDA Findings

Decision #284

[2004] C.P.C.S.F. No. 41 (QL)

Use and Disclosure of Health Information Inappropriate
(November 30, 2004)

Principles 4.3, 4.3.5, Schedule 1;
Sections 5(3), 8(3), 8(5) and para. 9(3)(*d*)

Complaint/Investigation

An employee of a telecommunications company complained (at para. 1):

1. *that her employer used and disclosed her personal information without her consent...;*
2. *that her employer denied her access to her personal information.*

Since the employer is self-insuring, if an employee's absence exceeds a specified period, a physician's report is required. On the doctor's form, the employee authorizes the doctor to release information to the company's health unit. The director of the health unit is a doctor. The health unit assesses an employee's ability to return to work, eligibility for benefits, and to determine the company's obligations to the employee under human rights legislation. This unit safeguards employee information quite strictly, and members of the unit sign a confidentiality agreement. The only information that is disclosed to the employee's manager pertains to the employee's eligibility for benefits and ability to return to work, workplace accommodations to support such a return, and/or the employee's prognosis.

The complainant left work after an argument with her supervisor, citing a medical condition as her reason. After receiving her doctor's report, the unit required the complainant to undergo an independent medical examination. The doctor found that the complainant was not disabled, therefore her benefits were suspended and she was directed to return to work.

After looking at the independent examiner's report, the complainant noted that it mentioned interactions with her, her manager and to health records relating to two previous absences. The complainant did not believe that

the previous absences were relevant to her current absence, and did not disclose this information to the doctor. The complainant thought that it was wrong for her manager to share this information with the doctor without her consent. The company claimed that it was vital that the independent medical examiner have a complete picture of the employee's medical history. The information that was disclosed to the medical examiner was screened for its relevance.

With respect to the second complaint, the company claimed that it keeps three to four files on each employee. One file is kept with the health unit, the district office maintains a personnel file, an employee's manager keeps a binder on each employee, and industrial relations consultants may keep a file if relevant.

The complainant had filed an access request that was responded to 22 days later. The complainant was informed that she was receiving a copy of her personnel file, with the exception of some documents, pursuant to para. 9(3)(*d*) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA). The complainant's grievance pertained to those particular documents. The complainant also requested information from the health unit. She had received copies of two e-mails that led her to believe that her managers had withheld some information to which she should have had access.

Findings

With respect to the use and disclosure complaint, the Assistant Privacy Commissioner noted that a reasonable person would likely consider the collection and disclosure of employee personal information reasonable in the circumstances. Further, the managers shared some information concerning the circumstances surrounding the complainant's absence from work. The Assistant Privacy Commissioner found that this information was directly relevant to the company's determination of the complainant's ability to return to work and her eligibility for continuing employee benefits. The complainant was aware of the purpose for the medical examination. Accordingly, she should have surmised that some information would be provided to the examiner to inform him about the circumstances surrounding the absence, and that she had been absent before with an identical diagnosis.

The Assistant Privacy Commissioner found that the complainant had impliedly consented to the use and disclosure of her personal information. It should have been expected that information related to her absence and eligibility to receive benefits would be used and disclosed. Organizations should be obliged to obtain the express consent of employees only when the contemplated use or disclosure might not be reasonably anticipated in the circumstances, or is a new purpose that has not been previously communicated to employees. With this in mind, the company had acted in compliance with principles 4.3, 4.3.5, and s. 5(3). The use and disclosure complaint was not well-founded.

With respect to the denial of access complaint, the Assistant Privacy Commissioner found that the complainant did not receive a copy of her district file until 243 days after the access request. By exceeding the time limit prescribed in s. 8(3), the company was deemed to have refused the access request, contrary to s. 8(5). The company appropriately applied para. 9(3)(*d*) to the documents generated after the complainant filed her grievances. The company, however, applied the same exemption to some material created before her complaint. This information could not be deemed to have been generated in the course of a formal dispute resolution process. Since the company incorrectly applied the exemption to this material, the denial of access complaint was well-founded.

Further Considerations

The Assistant Privacy Commissioner recommended that the company: (a) release the information that it had incorrectly withheld under paragraph 9(3)(d); and (b) review its access procedures with the managers who dealt with the access request.

Decision #287

[2005] C.P.C.S.F. No. 1 (QL)

Request for Medical Information Deemed to be Reasonable, Although Consent Procedures Improper (January 5, 2005)

Principles 4.3, 4.4.1, Schedule 1; Subsection 5(3)

Complaint/Investigation

An employee of a transportation company claimed: (i) that his employer required him to provide more medical information than was necessary and would not

permit him to return to his position until the information was supplied; and (2) that the company acquired medical information about him from his doctor without his consent.

After recovering from a serious illness, the complainant returned to his position with his employer. When the complainant returned to work, a medical examination determined that he was fit for light work only. One year after he had returned to work, the company informed the complainant that because of the position he occupied, he was required to provide medical information that guaranteed that he was not at risk of sudden incapacity. The Office of the Privacy Commissioner reviewed the documentation that was sent to the complainant and his physician and established the following:

- The company asked the complainant to have his doctor complete two forms updating his medical condition.
- The complainant's doctor completed both forms. The complainant did not sign the consent clause that was located at the top of both forms. Nonetheless, the physician completed the forms and sent them back. When the company found that information was missing, it wrote to the complainant. No results of a particular test related to the complainant's condition were attached to the form, therefore the company requested that the complainant contact the doctor. Since the complainant never forwarded this request to the doctor, the company doctor contacted the specialist directly by phone to obtain a copy of the test.

The complainant was informed that if he did not provide the requested information he would be restricted from performing his work duties. He eventually received a note from his new specialist, indicating that he was fit to work. The company, however, was not satisfied with this response, and restricted the complainant to working in non-safety sensitive positions.

Findings

Concerning the claim that the employer required the complainant to provide excessive personal information, the Assistant Privacy Commissioner noted the company's purpose for collecting this information was to guarantee the safety of employees. The company wanted the complainant to provide some follow-up information due to his health problems and because he occupied a safety-sensitive position. This purpose appeared to be appropriate in the circumstances, and was in compliance with s. 5(3). The company had also limited its collection to what was necessary to fulfill this purpose, in accordance with principle 4.4.1.

The Assistant Privacy Commissioner considered the claim that the company had collected medical information about the complainant without his consent to have merit. The problem occurred when the company had additional questions for the specialist and contacted him directly. The company should not have obtained this information directly from the specialist as it did not have the valid signed consent form from the complainant authorizing the company to speak to the specialist. Accordingly, the Assistant Privacy Commissioner found that the company collected some medical information about the complainant without his consent, contrary to principle 4.3.

The allegation that the company was requiring the complainant to provide excessive medical information was not well-founded, however, the claim that the company collected personal information without consent was well-founded.